

# ***Защита в операционных системах***

Вязанкин Олег Николаевич

к.ф.-м.н., доцент кафедры ПОЗИ, ИМИТ

[ovyazankin@gmail.com](mailto:ovyazankin@gmail.com)



## Тема 6. Домены Windows.



# План

- Общие сведения
- Сквозная аутентификация
- Отношения доверия
- Активный каталог
- Групповая политика
- Заключение

# Общие сведения

Современные сети часто состоят из множества различных программных платформ, большого разнообразия оборудования и программного обеспечения. Пользователи зачастую вынуждены запоминать большое количество паролей для доступа к различным сетевым ресурсам. Права доступа могут быть различными для одного и того же сотрудника в зависимости от того, с какими ресурсами он работает. Все это множество взаимосвязей требует от администратора и пользователя огромного количества времени на анализ, запоминание и обучение.

Решение проблемы управления такой разнородной сетью было найдено с разработкой службы каталога. Службы каталога предоставляют возможности управления любыми ресурсами и сервисами из любой точки независимо от размеров сети, используемых операционных систем и сложности оборудования. Информация о пользователе, заносится единожды в службу каталога, и после этого становится доступной в пределах всей сети. Адреса электронной почты, принадлежность к группам, необходимые права доступа и учетные записи для работы с различными операционными системами — все это создается и поддерживается в актуальном виде автоматически. Любые изменения, занесенные в службу каталога администратором, сразу обновляются по всей сети.

В настоящее время большинство служб каталогов различных фирм базируются на стандарте X.500. Для доступа к информации, хранящейся в службах каталогов, обычно используется протокол *Lightweight Directory Access Protocol* ( *LDAP* ). В связи со стремительным развитием сетей TCP/IP, протокол LDAP становится стандартом для служб каталогов и приложений, ориентированных на использование службы каталога.



# Общие сведения

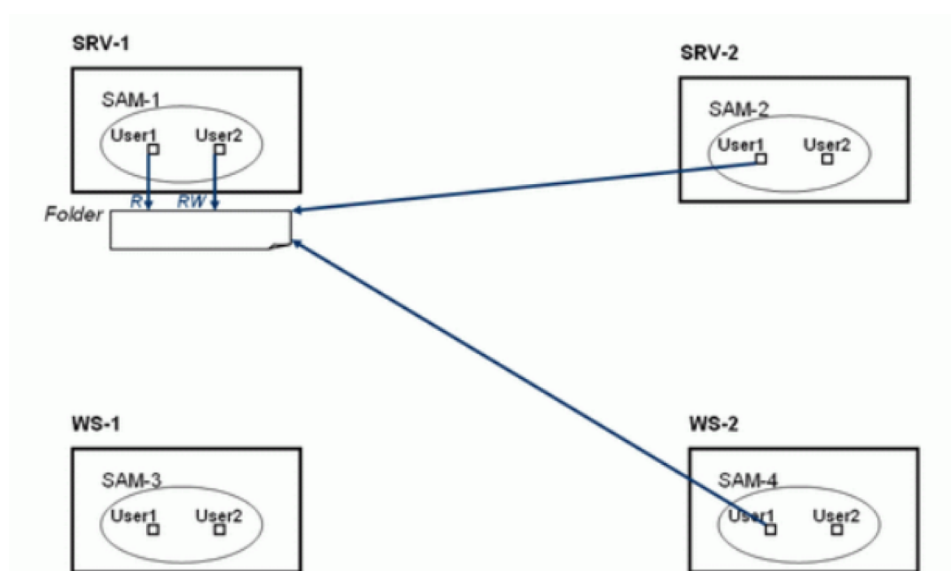
Служба каталогов Active Directory является основой логической структуры корпоративных сетей, базирующихся на ОС Windows. Термин «Каталог» в самом широком смысле означает «Справочник», а служба каталогов корпоративной сети — это централизованный корпоративный справочник. Корпоративный каталог может содержать информацию об объектах различных типов. Служба каталогов Active Directory содержит в первую очередь объекты, на которых базируется система безопасности сетей Windows, — учетные записи пользователей, групп и компьютеров. Учетные записи организованы в логические структуры: домен, дерево, лес, организационные подразделения.

# Общие сведения

## Модели управления безопасностью. Модель «Рабочая группа»

Данная модель управления безопасностью корпоративной сети — самая примитивная. Она предназначена для использования в небольших одноранговых сетях (3–10 компьютеров) и основана на том, что каждый компьютер в сети с операционными системами Windows имеет свою собственную локальную базу данных учетных записей и с помощью этой локальной БД осуществляется управление доступом к ресурсам данного компьютера. Локальная БД учетных записей называется база данных SAM ( Security Account Manager ) и хранится в реестре ОС. Базы данных отдельных компьютеров полностью изолированы друг от друга и никак не связаны между собой.

Пример управления доступом при использовании такой модели изображен на рисунке.



# Общие сведения

## Модели управления безопасностью. Модель «Рабочая группа»

В данном примере изображены два сервера (SRV-1 и SRV-2) и две рабочие станции (WS-1 и WS-2). Их базы данных SAM обозначены соответственно SAM-1, SAM-2, SAM-3 и SAM-4 (на рисунке базы SAM изображены в виде овала).

В каждой БД есть учетные записи пользователей User1 и User2. Полное имя пользователя User1 на сервере SRV-1 будет выглядеть как "SRV-1\User1", а полное имя пользователя User1 на рабочей станции WS-1 будет выглядеть как "WS-1\User1".

Представим, что на сервере SRV-1 создана папка Folder, к которой предоставлен доступ по сети пользователям User1 — на чтение (R), User2 — чтение и запись (RW). Главный момент в этой модели заключается в том, что компьютер SRV-1 ничего "не знает" об учетных записях компьютеров SRV-2, WS-1, WS-2, а также всех остальных компьютеров сети. Если пользователь с именем User1 локально регистрируется в системе на компьютере, например, WS-2 (или, как еще говорят, "войдет в систему с локальным именем User1 на компьютере WS-2"), то при попытке получить доступ с этого компьютера по сети к папке Folder на сервере SRV-1 сервер запросит пользователя ввести имя и пароль (исключение составляет тот случай, если у пользователей с одинаковыми именами одинаковые пароли).



# Общие сведения

## Модели управления безопасностью. Модель «Рабочая группа»

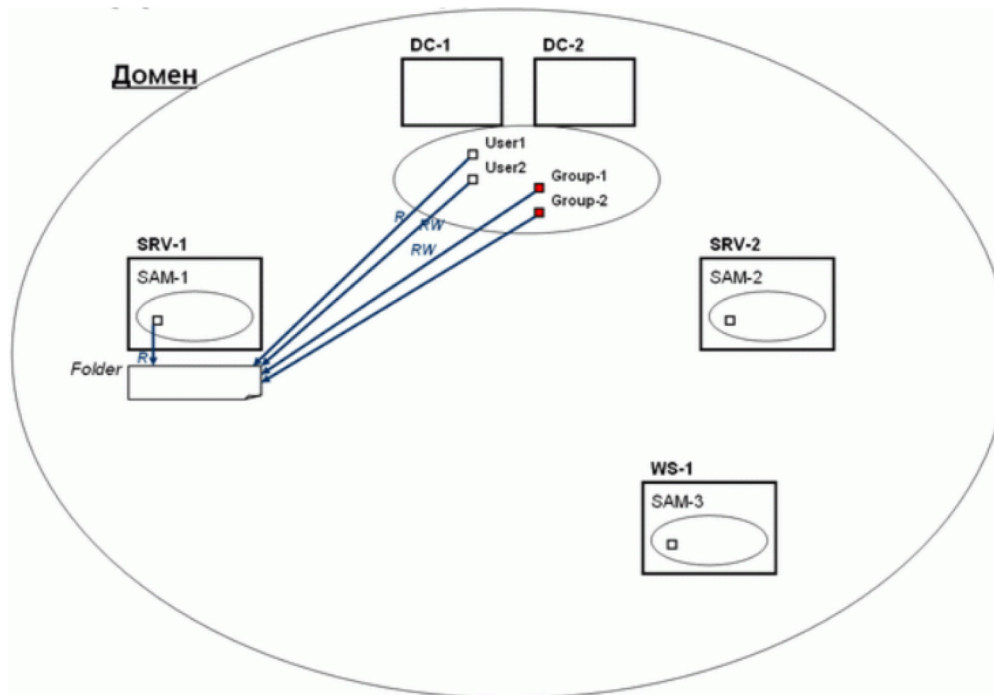
При использовании в сети с большим количеством компьютеров и сетевых ресурсов становится очень сложным управлять именами пользователей и их паролями — приходится на каждом компьютере (который предоставляет свои ресурсы для совместного использования в сети) вручную создавать одни и те же учетные записи с одинаковыми паролями, что очень трудоемко, либо делать одну учетную запись на всех пользователей с одним на всех паролем (или вообще без пароля), что сильно снижает уровень защиты информации. Поэтому модель "Рабочая группа" рекомендуется только для сетей с числом компьютеров от 3 до 10 (а еще лучше — не более 5), при условии что среди всех компьютеров нет ни одного с системой Windows Server.



# Общие сведения

## Модели управления безопасностью. Доменная модель

В доменной модели существует единая база данных служб каталогов, доступная всем компьютерам сети. Для этого в сети устанавливаются специализированные серверы, называемые *контроллерами домена*, которые хранят на своих жестких дисках эту базу. На рисунке изображена схема доменной модели. Серверы DC-1 и DC-2 — контроллеры домена, они хранят доменную базу данных учетных записей (каждый контроллер хранит у себя свою собственную копию БД, но все изменения, производимые в БД на одном из серверов, реплицируются на остальные контроллеры).



# Общие сведения

## Модели управления безопасностью. Доменная модель

В такой модели, если, например, на сервере SRV-1, являющемся членом домена, предоставлен общий доступ к папке Folder, то права доступа к данному ресурсу можно назначать не только для учетных записей локальной базы SAM данного сервера, но, самое главное, учетным записям, хранящимся в доменной БД. На рисунке для доступа к папке Folder даны права доступа одной локальной учетной записи компьютера SRV-1 и нескольким учетным записям домена (пользователя и группам пользователей).

В доменной модели управления безопасностью пользователь регистрируется на компьютере ("входит в систему") со своей доменной учетной записью и, независимо от компьютера, на котором была выполнена регистрация, получает доступ к необходимым сетевым ресурсам. И нет необходимости на каждом компьютере создавать большое количество локальных учетных записей, все записи созданы однократно в доменной БД. И с помощью доменной базы данных осуществляется централизованное управление доступом к сетевым ресурсам независимо от количества компьютеров в сети.

Основной задачей, для решения которой предназначена доменная архитектура компьютерной сети, является упрощение администрирования и управления сетью.

# Общие сведения

Далее рассмотрим некоторые понятия доменной модели.

*Доменом* называется совокупность компьютеров, объединенных в общую сеть и разделяющих общий список пользователей и общую политику безопасности.

В сравнении с рабочими группами домены – это группы безопасности, имеющие единую базу регистрации, тогда как рабочие группы – это всего лишь логическое объединение машин. Имена доменов формируются по той же схеме, что и имена в пространстве имен DNS. И это не случайно. Служба DNS является средством поиска компонент.

Иерархическая система доменов, имеющая единый корень (корневой домен), называется *деревом доменов*.

Корпорация Microsoft рекомендует строить сеть в виде одного домена. Построение дерева, состоящего из многих доменов необходимо в следующих случаях:

- для децентрализации администрирования служб каталогов (например, в случае, когда компания имеет филиалы, географически удаленные друг от друга, и централизованное управление затруднено по техническим причинам);
- для повышения производительности (для компаний с большим количеством пользователей и серверов актуален вопрос повышения производительности работы контроллеров домена);
- для более эффективного управления репликацией (если контроллеры доменов удалены друг от друга, то репликация в одном может потребовать больше времени и создавать проблемы с использованием несинхронизированных данных);
- для применения различных политик безопасности для различных подразделений компании;
- при большом количестве объектов в БД Active Directory.

# Общие сведения

Множество деревьев доменов, находящихся в различных формах доверительных отношений образуют *лес доменов* (см. раздел «Отношения доверия»).

Лес объединяет деревья, которые поддерживают единую схему ( *схема Active Directory* — набор определений типов, или классов, объектов в БД Active Directory). По умолчанию, первый домен, создаваемый в лесу, считается его корневым доменом, в корневом домене хранится схема AD.

Новые деревья в лесу создаются в том случае, когда необходимо построить иерархию доменов с пространством имен, отличным от других пространств леса.

При работе с лесами и деревьями необходимо помнить следующее:

- первое созданное в лесу *доменов дерево* является *корневым деревом*, первый созданный в дереве домен называется *корневым доменом дерева* ( *tree root domain* );
- первый домен, созданный в лесу доменов, называется *корневым доменом леса* ( *forest root domain* ), данный домен не может быть удален (он хранит информацию о конфигурации леса и деревьях доменов, его образующих);
- нельзя добавить в дерево уже существующий домен;
- нельзя включить в лес уже существующее дерево;
- если домены помещены в лес, их невозможно переместить в другой лес;
- нельзя удалить домен, имеющий дочерние домены.

# Общие сведения

Учетная информация о пользователях, псевдопользователях и группах домена централизованно хранится в единой базе данных. Наличие общей базы учетных записей позволяет пользователю, единожды войдя в домен, осуществлять доступ к любому разделяемому ресурсу данного домена.

Однако, надо иметь в виду, что большинство возможностей, предоставляемых доменной архитектурой, могут быть отключены для отдельных компьютеров или пользователей. Далее везде под словами «пользователь может выполнить некоторое действие» подразумевается «пользователь может выполнить некоторое действие, если эта возможность не отключена явно». Если на пользователя не наложены специальные ограничения, он может подключаться к домену с любого компьютера сети.

Компьютеры, входящие в домен и работающие под управлением Windows, могут управляться централизованно. Большинство задач администрирования могут выполняться администратором домена со своего рабочего места в отношении любого компьютера домена. В частности, администратор домена может выполнять на любом компьютере домена следующие действия:

- создавать, удалять, переименовывать и менять атрибуты разделяемых каталогов и принтеров;
- просматривать и редактировать реестр;
- создавать, удалять, загружать и выгружать драйверы и сервисы;
- просматривать системные журналы, включая журнал аудита.



# Общие сведения

Одним из важнейших элементов доменной архитектуры Windows является база учетных записей, в которой централизованно хранится информация о пользователях, псевдопользователях и группах домена. Каждому компьютеру домена соответствует псевдопользователь с именем `computer_name$`, учетная информация компьютера хранится в базе в таком же формате, как и учетная информация пользователя.

# Общие сведения

## Контроллер домена

В каждом домене Windows обязательно существует хотя бы один сервер, называемый *контроллером домена (domain controller, DC)*. База учетных записей домена физически хранится на жестком диске этого компьютера: в Windows NT — в реестре, начиная с Windows 2000 — в специальной базе данных, называемой *активным каталогом*. В роли контроллера домена может выступать только Windows Server, рабочие станции контроллерами доменов быть не могут.

В домене может существовать более одного контроллера, в этом случае все контроллеры домена хранят идентичные копии (реплики) базы учетных записей домена. Время от времени в домене выполняется синхронизация реплик базы учетных записей, хранящихся на разных контроллерах домена.

В Windows NT среди контроллеров домена выделялся один *первичный контроллер*, хранящий эталонную копию базы учетных записей. Начиная с Windows 2000, все контроллеры домена равноправны, для синхронизации разных копий базы учетных записей используются развитые средства репликации данных.

Членами домена могут быть любые компьютеры, операционные системы которых способны взаимодействовать с контроллерами домена. В полном объеме преимуществами доменной архитектуры могут пользоваться только компьютеры, работающие под управлением Windows 2000 или выше, однако отдельные функции доменной архитектуры могут использоваться любыми компьютерами, программное обеспечение которых способно осуществлять информационный обмен по сетевому протоколу SMB.

# Сквозная аутентификация

Когда пользователь начинает работу с операционной системой Windows, входящей в состав домена, пользователь указывает в соответствующем поле формы ввода домен, в котором зарегистрирована учетная запись.

- Если пользователь указал в качестве домена имя локального компьютера, вход в домен не производится, аутентификация выполняется с использованием локальной базы учетных записей и пользователь работает с операционной системой, как если бы рабочая станция представляла собой изолированный компьютер. В дальнейшем всякий раз, когда пользователь захочет обратиться к ресурсам другого компьютера того же домена, пользователь должен будет пройти повторную аутентификацию.
- Если же пользователь, входя в систему, указал, что его учетная запись зарегистрирована в домене, операционная система выполняет *сквозную* или *транзитную аутентификацию*. Сквозную аутентификацию может осуществлять не только Windows, но и любая другая операционная система, в состав которой входит соответствующий сетевой клиент.
- Если пользователь не указал, где зарегистрирована его учетная запись, операционная система вначале пытается провести локальную аутентификацию, а если учетная запись пользователя отсутствует в локальной базе — сквозную.



# Сквозная аутентификация

## Алгоритм сквозной аутентификации

Сквозная аутентификация выполняется следующим образом.

1. Рабочая станция устанавливает сетевое соединение с контроллером домена. Если ни один контроллер домена недоступен, сквозная аутентификация невозможна.
2. Осуществляется взаимная аутентификация рабочей станции и контроллера домена. Псевдопользователь, соответствующий рабочей станции, проходит аутентификацию на контроллере домена, а псевдопользователь, соответствующий контроллеру домена, проходит аутентификацию на рабочей станции. Если взаимная аутентификация компьютеров невозможна (например, если контроллер домена подменен нарушителем), сквозная аутентификация пользователя также невозможна.
3. Рабочая станция и контроллер домена договариваются о протоколе, по которому будет передаваться идентификационная и аутентификационная информация аутентифицирующегося пользователя. Если договориться невозможно (например, если в домене запрещена открытая передача по сети аутентификационной информации, а программное обеспечение рабочей станции не поддерживает шифрование паролей), сквозная аутентификация невозможна.
4. Идентификационная и аутентификационная информация пользователя, проходящего аутентификацию, пересылается контроллеру домена. Если в домене используется протокол аутентификации Kerberos (начиная с Windows 2000, он используется почти всегда), данный шаг алгоритма включает в себя длинную и нетривиальную последовательность запросов и ответов, при этом используется весьма сложное шифрование.
5. Контроллер домена проводит аутентификацию пользователя с использованием данных, хранящихся в базе учетных записей домена. Если аутентификация прошла неуспешно (например, пользователь ввел неверный пароль или пользователю запрещено входить в домен с данного компьютера), рабочая станция получает от контроллера домена отрицательный ответ и аутентификация прерывается.
6. Если аутентификация прошла успешно, контроллер домена высылает рабочей станции учетную информацию пользователя, необходимую для формирования его маркера доступа. Рабочая станция формирует маркер доступа и на этом аутентификация завершается.

# Сквозная аутентификация

## Алгоритм сквозной аутентификации

Из вышеприведенного алгоритма видно, что сквозная аутентификация в доменах Windows защищена от навязывания нарушителем ложного сервера. Если нарушитель каким-то образом отключит от сети контроллер домена и подключит вместо него свой компьютер, отвечающий на те же запросы, рабочая станция распознает подмену, поскольку компьютер нарушителя не сможет пройти взаимную аутентификацию компьютеров (чтобы это стало возможным, нарушитель должен иметь доступ к базе учетных записей домена, а тогда отпадает необходимость в данной атаке).

Единственное, что нарушитель может навязать рабочей станции и контроллеру домена, реализующим сквозную аутентификацию некоторого пользователя, — выбор алгоритма, по которому аутентификационная информация пользователя будет передаваться по сети. Если в обеих операционных системах, участвующих в информационном обмене, нет никаких ограничений на алгоритм передачи аутентификационной информации, нарушитель может спровоцировать передачу пароля по сети в открытом виде, без шифрования. Однако начиная с Windows NT 4.0 SP4, открытая передача пароля по сети по умолчанию запрещена. Самое большее, чего может добиться нарушитель в таких системах — заставить рабочую станцию отправить аутентификационную информацию по устаревшему протоколу LanMan, более уязвимому в отношении подбора паролей. Однако начиная с Windows 2000 даже это, как правило, невозможно.

# Сквозная аутентификация

## Кэширование аутентификационной информации

Если ни один из контроллеров домена не в состоянии обслужить запрос рабочей станции, сквозная аутентификация невозможна. Этот факт существенно снижает устойчивость работы сети.

Для исключения подобных ситуаций в Windows поддерживается кэширование аутентификационной информации. После каждого успешного входа пользователя в домен аутентификационная информация пользователя сохраняется в зашифрованном виде в локальном реестре рабочей станции. В дальнейшем, когда пользователь пытается войти в систему и ни один из контроллеров домена не в состоянии выполнить сквозную аутентификацию, аутентификация пользователя осуществляется с использованием кэшированных аутентификационных данных.

Кэширование аутентификационной информации может быть отключено администратором операционной системы, поскольку оно снижает защищенность системы. Однако в большинстве случаев снижение защищенности аутентификационных данных пользователей от подбора вполне компенсируется повышением устойчивости работы сети.



# Сквозная аутентификация

## Группы пользователей

Так же, как и на отдельно стоящем компьютере Windows, в доменах Windows могут существовать группы пользователей. В группы пользователей домена (*глобальные группы*) могут входить только пользователи домена, пользователи отдельных компьютеров домена в группы домена входить не могут. Однако локальные группы отдельных компьютеров домена могут включать в себя пользователей домена и даже группы, зарегистрированные в домене.

Если локальная группа, зарегистрированная на некотором компьютере домена, включает в себя в качестве подгруппы глобальную группу, зарегистрированную в домене, то считается, что на данном компьютере все пользователи домена, входящие в глобальную группу, тем самым входят и в соответствующую локальную группу данного компьютера.

Список пользователей, входящих в локальную группу, составляется заново при каждой авторизации пользователя, этим гарантируется, что в маркер доступа авторизуемого пользователя будет внесена актуальная информация о его членстве в локальных и глобальных группах.

# Сквозная аутентификация

## Группы пользователей

Когда пользователь домена авторизуется на компьютере, входящем в состав домена, пользователь получает права и привилегии, предоставленные ему как:

- пользователю домена;
- члену локальных групп данного компьютера;
- члену глобальных групп домена;
- члену глобальных групп домена, являющихся подгруппами локальных групп данного компьютера.

Если пользователю на данном компьютере не назначены никакие полномочия, пользователь получает полномочия, предоставленные группе Everyone.

Описанная схема назначения полномочий позволяет гибко и централизованно управлять политикой безопасности в рамках всего домена. Например, если внести некоторого пользователя в группу домена Domain Admins, пользователь тем самым включается в группу Administrators на всех компьютерах домена, на которых группа Domain Admins является подгруппой группы Administrators (данное включение устанавливается по умолчанию при включении рабочей станции Windows в домен).

С другой стороны, если имеется необходимость реализовать на некотором компьютере домена политику безопасности, существенно отличающуюся от политики безопасности домена, это легко может быть сделано путем изменения порядка включения глобальных групп пользователей домена в локальные группы пользователей данного компьютера.

Начиная с Windows 2000, в группы могут включаться не только пользователи, но и компьютеры домена (фактически — псевдопользователи, соответствующие компьютерам).



# Сквозная аутентификация

## Группы пользователей

Помимо локальных групп пользователей, зарегистрированных на отдельных компьютерах, и глобальных групп, зарегистрированных в отдельных доменах, в лесу доменов Windows могут существовать так называемые *вселенские* группы. Вселенские группы определены в пределах всего леса, они могут использоваться при настройке политики безопасности на любом компьютере леса.

Также вселенские группы могут выступать в роли глобальных списков рассылки. Вселенские группы могут включать в себя пользователей, глобальные группы и другие вселенские группы. Включаться вселенские группы могут только в другие вселенские группы.

Таким образом, система групп Windows (локальные, глобальные и вселенские группы) позволяет описывать любые иерархические отношения между пользователями на любом из трех уровней: компьютера, домена и леса в целом.

# Отношения доверия

Между доменами Windows, функционирующими в одной физической сети, могут быть установлены *отношения доверия*. Если домен А доверяет домену В, это означает, что каждый пользователь домена В имеют доступ ко всем ресурсам домена А, за исключением тех ресурсов, доступ к которым явно запрещен данному конкретному пользователю.

В Windows NT отношения доверия были односторонними, т. е. из того, что домен А доверяет домену В, не следовало, что домен В доверяет домену А. Для того чтобы установить между доменами двусторонние отношения доверия, требовалось создать пару односторонних отношений доверия, направленных навстречу друг другу. Отношения доверия в Windows NT не были транзитивными, т. е. если домен А доверяет домену В, а домен В доверяет домену С, из этого не следовало, что домен А доверяет домену С.

Начиная с Windows 2000, домены могут быть объединены в единый лес, в котором все домены доверяют друг другу. Важно заметить, что Windows 2000 содержит развитые средства управления полномочиями пользователей в разных доменах и поэтому доверие всех всем вовсе не означает всеобщей вседозволенности, а означает лишь, что каждый пользователь имеет возможность обращаться ко всем ресурсам сети, к которым ему явно разрешен доступ.

При необходимости администратор леса доменов Windows 2000/2003/2008 может устанавливать и отношения доверия «в стиле NT», но на практике эта возможность почти не используется.

# Отношения доверия

Каждому домену в лесу соответствует псевдопользователь, используемый для взаимной аутентификации контроллерами доверяющих друг другу доменов. Любое обращение контроллера одного домена к контроллеру другого домена начинается с взаимной аутентификации этих компьютеров, что делает практически невозможной подмену контроллера домена и навязывание неверной информации контроллерам других доменов.

- В маленьком лесу каждый контроллер домена хранит у себя эталонный образ аутентификационных данных всех других контроллеров домена.
- В большом лесу каждый контроллер домена хранит у себя лишь аутентификационные данные «ближайших соседей», а взаимная аутентификация с контроллером «далекого» домена осуществляется путем выстраивания *цепочки*, состоящей из контроллеров доменов, при этом каждая пара соседних в цепочке контроллеров способна выполнить взаимную аутентификацию, не прибегая к посредничеству других компьютеров.



# Отношения доверия

Пусть пользователь домена А пытается войти в операционную систему рабочей станции, входящей в состав домена В, доверяющего домену А. Сквозная аутентификация в этом случае осуществляется следующим образом.

1. Рабочая станция устанавливает сетевое соединение с контроллером домена В.
2. Рабочая станция передает идентификационные и аутентификационные данные пользователя, входящего в систему, контроллеру домена В. Взаимная аутентификация рабочей станции и контроллера домена, а также выбор протокола передачи данных происходят точно так же, как и в случае сквозной аутентификации в одном домене.
3. Контроллер домена В передает идентификационные и аутентификационные данные пользователя контроллеру домена А (если необходимо, перед этим выполняется взаимная аутентификация контроллеров доменов А и В).
4. Контроллер домена А проводит аутентификацию пользователя с использованием информации, хранящейся в его базе учетных записей. Результаты аутентификации передаются контроллеру домена В.
5. Контроллер домена В перенаправляет результат аутентификации пользователя на рабочую станцию, с которой непосредственно работает пользователь.



# Отношения доверия

Если домен А доверяет домену В, то на каждом компьютере домена А права и привилегии могут назначаться следующим субъектам доступа:

- локальным пользователям, зарегистрированным на данном компьютере;
- локальным группам, зарегистрированным на данном компьютере;
- пользователям домена А;
- пользователям домена В;
- группам домена А;
- группам домена В.



# Активный каталог

Начиная с Windows 2000, иерархическая база учетных записей SAM преобразована в полнофункциональную распределенную базу данных, основанную на модели данных X.500 и называемую *активным каталогом* (*active directory, AD*).

В общем случае каталог — это база данных, оптимизированная для ситуации, когда обновления базы происходят много реже, чем получение информации из базы. Активный каталог Windows представляет собой частный случай общего понятия каталога.

На каждом контроллере домена хранится своя копия активного каталога, эти копии регулярно синхронизируются между собой. Место физического хранения файлов активного каталога указывается администратором в ходе установки сервисов активного каталога, в большинстве конфигураций предлагается путь по умолчанию %windir%\SYSVOL.

Информация, хранящаяся в активном каталоге, не ограничивается одними только учетными записями пользователей. В общем случае в активном каталоге могут храниться любые данные, структурированные в соответствии с требованиями формата базы данных.

# Активный каталог

## Объекты AD

Данные, хранящиеся в активном каталоге, рассматриваются как совокупность объектов, имеющих атрибуты (подобъекты), при этом набор атрибутов объекта определяется типом объекта. Подобъекты объекта могут содержать вложенные подобъекты, всего поддерживается пять уровней вложенности подобъектов (включая сам объект), однако в текущих версиях Windows используются только три уровня:

- объект;
- набор свойств (property set) — подобъект первого уровня;
- свойство (property) — подобъект второго уровня.

Среди объектов выделяются *контейнеры* — объекты, содержащие другие объекты. Объекты активного каталога образуют древовидную иерархическую структуру, подобную структуре файловой системы, в роли каталогов выступают контейнеры, а в роли файлов — объекты других типов.

Каждый объект активного каталога уникально идентифицируется 128-битным числовым идентификатором GUID. Кроме того, каждый объект имеет уникальное текстовое имя в специальном формате DN (distinguished name). DN однозначно идентифицирует объект, в активном каталоге не могут существовать два разных объекта, имеющих одинаковое DN. Для того чтобы обратиться к объекту, необязательно знать его DN, поиск объекта может быть осуществлен по части DN или по совокупности атрибутов объекта.



# Активный каталог

## Объекты AD

DN имеет вид:

**/атрибут=значение/атрибут=значение...**

Некоторые клиентские программы используют альтернативную запись DN:

**атрибу=значение, атрибут=значение...**

# Активный каталог

## Именованние пользователей домена

Начиная с Windows 2000, учетные записи пользователей и псевдопользователей хранятся в активном каталоге. Имя пользователя Windows может представляться в одном из следующих форматов:

- внутренний (DN) — /OU = организация/DC = DNS-домен/CN = Users/CN=имя\_пользователя;
  - OU (Organizational Unit) — указатель на организационное подразделение (ОП);
  - DC (Domain Component) — указатель на составную часть доменного имени;
  - CN (Common Name) — указатель на общее имя.
- Основной (UPN - User Principal Name) — имя\_пользователя@DNS-домен;
- совместимый с Windows NT — NetBIOS-домен\имя\_пользователя;
- сокращенный — имя\_пользователя.

Последние два формата не обеспечивают однозначную идентификацию пользователя. При использовании этих форматов осуществляется поиск в каталоге учетной записи пользователя, имеющего заданное имя, причем результатом поиска всегда является первая найденная запись (после нахождения первой записи поиск прекращается).

Нетрудно видеть, что основной формат имени пользователя Windows в точности совпадает с форматом, принятом в современных системах электронной почты. Это не является случайным совпадением. Список пользователей Windows весьма тесно интегрирован с электронной почтой и системами электронного документооборота.



# Активный каталог

## Глобальный каталог

Из выше изложенного можно заметить, что структура AD может быть весьма сложной и вмещать в себя большое количество объектов. Чего стоит только тот факт, что домен AD может включать в себя до 1,5 млн. объектов.

Но из-за этого могут возникнуть проблемы с производительностью при выполнении операций. Эта проблема решается с помощью *глобального каталога (Global Catalog, GC)*. Он содержит информацию о каждом объекте (хотя и не обо всех атрибутах этих объектов) всего леса AD, что помогает ускорять поиск объектов.

Глобальный каталог автоматически реплицируется на все контроллеры всех доверяемых доменов. Данные, лежащие в глобальном каталоге, доступны из любой точки любого доверяемого домена в любой момент времени (естественно, исключая фатальные сбои в функционировании сети). Владелец глобального каталога могут выступать специально назначенные для этого контроллеры домена.

# Активный каталог

## Доступ к AD

Для доступа к активному каталогу в Windows может использоваться либо специально разработанный в Microsoft протокол ADSI, либо протокол LDAP, использующийся для доступа к другим каталогам. Ряд функций активного каталога доступны также по протоколам MAPI-RPC и X.500.

В большом лесу запросы пользователей далекого домена могут проходить долгий путь. Для оптимизации путей прохождения запросов в лесах доменов Windows используется понятие *сайт*, или *узел (site)*.

В каждый сайт входят компьютеры, соединенные между собой высокоскоростными линиями связи. Компьютеры, входящие в одну подсеть протокола IP, всегда входят в один сайт. Внутри одного сайта репликация всегда осуществляется с использованием протокола RPC. Репликация между сайтами может происходить либо по RPC, либо с использованием одного из MAPI-протоколов (SMTP, X.400 и т. п.).

Как правило, сайт объединяет все компьютеры одного или нескольких доменов. Ситуаций, когда домен разбивается на два или более сайтов, рекомендуется избегать, поскольку это заметно ухудшает репликацию внутри домена.





# Активный каталог

## Доступ к AD

Для идентификации компьютеров в лесу используется протокол DNS, гарантирующий уникальность имен компьютеров в отличие от протокола NetBIOS, применявшегося для этой цели в Windows NT. Например, DNS-именам server.filial.xxx.ru и server.filial.xxx.ua соответствует общее NetBIOS-имя filial/server. Сервер DNS входит в состав дистрибутива Windows Server, обычно сервер DNS устанавливается на всех контроллерах доменов.

Любой объект активного каталога может быть защищен дескриптором защиты, имеющим такой же формат, как и дескриптор защиты локального объекта Windows.

Дескрипторы защиты объектов активного каталога наследуются по тем же правилам, что и дескрипторы защиты локальных объектов операционной системы. Для объектов активного каталога поддерживается атрибут «автоматическое наследование», позволяющий рекурсивно распространять делегирование полномочий пользователей на домены низших уровней.

# Групповая политика

Одним из важнейших новшеств в подсистеме защиты Windows является *групповая политика (group policy)* — совокупность объектов активного каталога, описывающих те или иные аспекты конфигурации операционной системы, а также индивидуальных настроек отдельных пользователей и групп. Групповая политика включает в себя большинство элементов политики безопасности Windows, в частности:

- распределение привилегий между пользователями;
- параметры подсистемы аутентификации, включая параметры протокола Kerberos;
- политику аудита;
- параметры системных журналов, включая журнал аудита;
- параметры сервисов, включая режим запуска (автоматический/ ручной/запуск запрещен) и дескриптор защиты сервиса;
- список агентов восстановления EFS;
- шаблоны настроек отдельных прикладных и системных программ (Internet Explorer, Task Scheduler, Windows Installer и т.п.).

В типичных конфигурациях Windows групповая политика содержит около 200-400 элементов. Для удобства администрирования они объединены в древовидную иерархическую структуру контейнеров.

Каждый компьютер, работающий под управлением Windows, имеет собственную групповую политику. Исключение составляют контроллеры доменов, которые разделяют между собой общую групповую политику, единую для всех контроллеров одного домена. Также существует единая групповая политика для всего домена в целом.



# Групповая политика

## Организационные единицы

В домене могут быть выделены особые группы пользователей и компьютеров, называемые *организационными единицами (organizational units)*.

Организационные единицы отличаются от обычных групп тем, что им могут назначаться собственные групповые политики. Это позволяет одновременно назначать одинаковые настройки всем компьютерам, входящим в состав одной организационной единицы. Тем самым организационные единицы упрощают администрирование большой сети.

Организационные единицы могут включаться одна в другую, групповые политики вышележащих организационных единиц наследуются нижележащими организационными единицами. Также групповые политики могут назначаться сайтам.

Каждый элемент групповой политики может быть либо не определен, либо иметь некоторое значение. Тип и диапазон возможных значений различаются для разных элементов групповой политики.

Значение элемента групповой политики, определенное в некоторой организационной единице, автоматически наследуется всеми нижележащими организационными единицами.

# Групповая политика

## Организационные единицы

Если значение элемента групповой политики, унаследованное от групповой политики вышележащей организационной единицы, вступает в противоречие с значением того же элемента, определенного в нижележащей организационной единице, то конфликт разрешается по следующим правилам:

- если администраторы обеих организационных единиц не указали никаких особых правил разрешения данного конфликта, то действует унаследованное значение;
- если администратор нижележащей организационной единицы установил на данную групповую политику флаг «не наследовать сверху», а администратор вышележащей организационной единицы не установил порядок разрешения данного конфликта, то действует значение, определенное администратором нижележащей организационной единицы;
- если администратор вышележащей организационной единицы установил на данную групповую политику флаг «наследовать вниз в любом случае», то унаследованное значение данного элемента групповой политики действует в любом случае, независимо от того, что определил в отношении данного элемента администратор нижележащей организационной единицы.



# Групповая политика

## Организационные единицы

Групповая политика позволяет администраторам организационных единиц централизованно управлять политикой безопасности большой сети. Если есть необходимость изменить некоторый аспект политики безопасности всего дерева, администратору корня дерева достаточно всего лишь настроить соответствующим образом групповую политику корня дерева и внесенные им изменения будут автоматически реплицированы на все компьютеры дерева.

При этом администраторы нижележащих организационных единиц, несогласные с решением более высокого администратора, могут (если это явно не запрещено администратором вышележащей организационной единицы) отменить это решение в части, касающейся подведомственных им организационных единиц леса.

Обычно администраторы организационных единиц высокого уровня оставляют большинство полей групповой политики незаполненными. Это дает администраторам организационных единиц низшего уровня свободу выбора в настройке политики безопасности своих организационных единиц.

# Групповая политика

## Организационные единицы

Элементы групповой политики сгруппированы в древовидную иерархическую структуру, аналогичную структуре файловой системы или реестра. Групповая политика, назначенная компьютеру, домену, организационной единице или сайту, включает в себя два больших раздела:

- Computer Configuration (конфигурация компьютера) — содержит политики, действующие на всю операционную систему в целом;
- User Configuration (конфигурация пользователя) — содержит политики, действующие на индивидуальные настройки пользователей, работающих с данным компьютером.

Пользователям и группам, не являющимся организационными единицами, может назначаться «неполноценная» групповая политика, содержащая только раздел User Configuration. Эта групповая политика считается более высокоприоритетной, чем групповая политика компьютера.

# Групповая политика

## Организационные единицы

Каждый из двух разделов групповой политики распадается на три подраздела:

- Software Settings — содержит политики, используемые сторонним программным обеспечением, не входящим в состав дистрибутива Windows. Чаще всего этот подраздел пуст;
- Windows Settings — содержит политики, описывающие настройки различных компонент Windows. Большинство политик, содержащихся в данном подразделе, связаны с безопасностью операционной системы;
- Administrative Templates — содержит политики, позволяющие автоматизировать управление большой сетью, применяя одни и те же настройки к разным компьютерам сети. В отличие от подраздела Windows Settings, в подразделе Administrative Templates по умолчанию все политики не определены. Администратор может определять эти политики либо вручную, с помощью консоли администрирования Windows (MMC), либо с использованием заранее подготовленных файлов административных шаблонов (ADM-файлов).

# Заключение

В заключении отметим те преимущества, которые мы получаем, отказываясь от одноранговой сети с использованием рабочих групп в пользу доменной модели.

- **Единая точка аутентификации.** В рабочей группе на каждом компьютере или сервере придётся вручную добавлять полный список пользователей, которым требуется сетевой доступ. Если вдруг один из сотрудников захочет сменить свой пароль, то его нужно будет поменять на всех компьютерах и серверах. Хорошо, если сеть состоит из 10 компьютеров, но если их больше? При использовании домена Active Directory все учётные записи пользователей хранятся в одной базе данных, и все компьютеры обращаются к ней за авторизацией. Все пользователи домена включаются в соответствующие группы, например, «Бухгалтерия», «Финансовый отдел». Достаточно один раз задать разрешения для тех или иных групп, и все пользователи получают соответствующий доступ к документам и приложениям. Если в компанию приходит новый сотрудник, для него создаётся учётная запись, которая включается в соответствующую группу, – сотрудник получает доступ ко всем ресурсам сети, к которым ему должен быть разрешён доступ. Если сотрудник увольняется, то достаточно заблокировать – и он сразу потеряет доступ ко всем ресурсам (компьютерам, документам, приложениям).
- **Единая точка управления политиками.** В рабочей группе все компьютеры равноправны. Ни один из компьютеров не может управлять другим, невозможно проконтролировать соблюдение единых политик, правил безопасности. При использовании единого каталога Active Directory, все пользователи и компьютеры иерархически распределяются по организационным подразделениям, к каждому из которых применяются единые групповые политики. Политики позволяют задать единые настройки и параметры безопасности для группы компьютеров и пользователей. При добавлении в домен нового компьютера или пользователя, он автоматически получает настройки, соответствующие принятым корпоративным стандартам. При помощи политик можно централизованно назначить пользователям сетевые принтеры, установить необходимые приложения, задать параметры безопасности браузера, настроить приложения Microsoft Office.



# Заключение

- **Повышенный уровень информационной безопасности.** Использование служб Active Directory значительно повышает уровень безопасности сети. Во-первых – это единое и защищённое хранилище учётных записей. В доменной среде все пароли доменных пользователей хранятся на выделенных серверах контроллерах домена, которые, как правило, защищены от внешнего доступа. Во-вторых, при использовании доменной среды для аутентификации используется протокол Kerberos, который значительно безопаснее, чем NTLM, использующийся в рабочих группах.
- **Интеграция с корпоративными приложениями и оборудованием.** Большим преимуществом служб Active Directory является соответствие стандарту LDAP, который поддерживается другими системами, например, почтовыми серверами (Exchange Server), прокси-серверами (ISA Server, TMG). Причем это не обязательно только продукты Microsoft. Преимущество такой интеграции заключается в том, что пользователю не требуется помнить большое количество логинов и паролей для доступа к тому или иному приложению, во всех приложениях пользователь имеет одни и те же учётные данные – его аутентификация происходит в едином каталоге Active Directory. Windows Server для интеграции с Active Directory предоставляет протокол RADIUS, который поддерживается большим количеством сетевого оборудования. Таким образом, можно, например, обеспечить аутентификацию доменных пользователей при подключении по VPN извне, использование Wi-Fi точек доступа в компании.
- **Единое хранилище конфигурации приложений.** Некоторые приложения хранят свою конфигурацию в Active Directory, например, Exchange Server. Развёртывание службы каталогов Active Directory является обязательным условием для работы этих приложений. Хранение конфигурации приложений в службе каталогов является выгодным с точки зрения гибкости и надёжности. Например, в случае полного отказа сервера Exchange, вся его конфигурация останется нетронутой. Для восстановления работоспособности корпоративной почты, достаточно будет переустановить Exchange Server в режиме восстановления.